Problem Set 3

1. The following cipher alphabet was constructed using a keyword columnar transposition scheme. What was the keyword used?
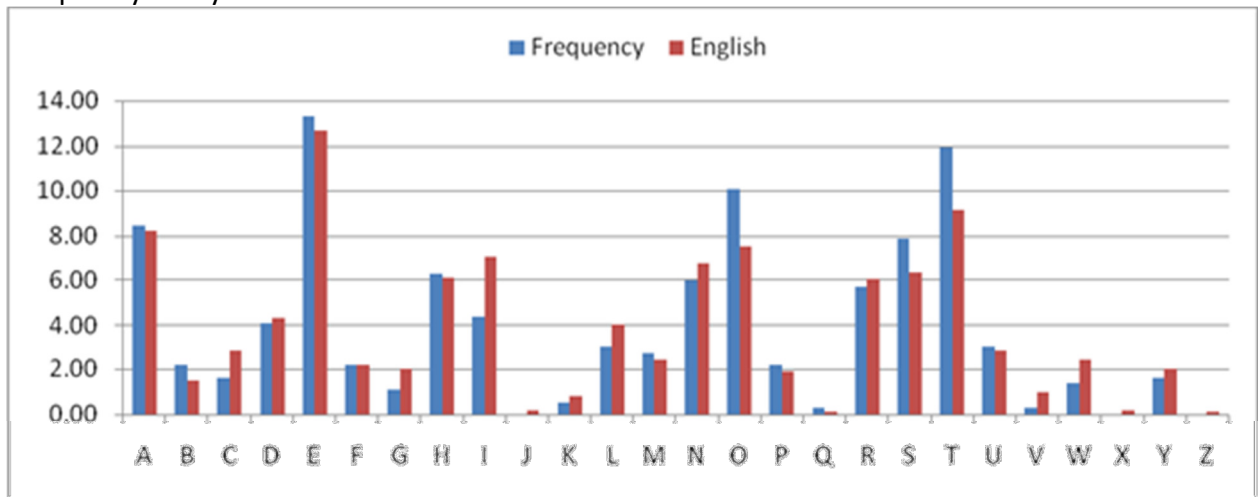
B   C   L   V   A   D   M   W   I   E   P   X   N   F   Q   Y   G   H   R   Z   T   J   S   O   K   U

2. Decipher the following. Then determine how the cipher alphabet was constructed. Be sure to identify any keywords. You should assume that a monoalphabetic substitution cipher was used.
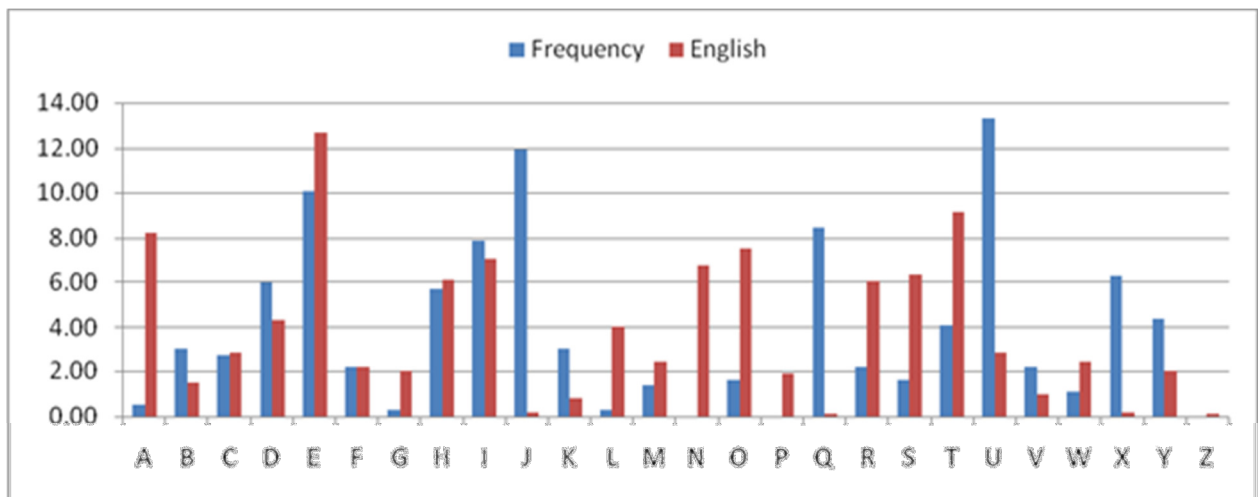
DJQCT JKNQC TNJON DQDPC DPHTP QCTST HQDSQ NDOTP GJKWJ RPQCT LDSQP SKTXD PQTEA
KNSTJ QUNDT PRHKJ BPDET HDQTN RQTSU HQUNT PPUSC RPQCT NKIRJ PQCTD NDPCR JEQCT
RJBHK PRXKJ PQCTY WTNTQ CTKEE PKSDT QYKUQ DJQCR QQCTY EDEJQ HTRVT RJYWN DQQTJ
NTSKN EPRYP NKOHT TKAQC TUJDV TNPDQ YKATX TQTND JTJBH RJEPR VTAKN PKITI YPQTN
DKUPH KKGDJ BPTQP KAPYI OKHPK JPQKJ TPRJE FTWTH PHTTR JECDP SKWKN GTNPJ KWSHR
DIQCR QQCTP YIOKH PRNTW NDQQT JHRJB URBTL TNCRL PQCTL DSQPW TNTJK QDHHD QTNRQ
TRAQT NRHHH TTPQT RIRQQ RSGTE QCTLN KOHTI WDQCI RQCWN DQQTJ HRJBU RBTPR NTEDP
QDJBU DPCRO HTANK INRJE KIPTM UTJST PKAPY IOKHP OTSRU PTQCT YSKJQ RDJPK ITPQR
QDPQD SRHLN TEDSQ RODHD QYQCT LRLTN PCKWP QCRQQ CTLDS QDPCP YIOKH PRNTS
CRNRS QTNPK ARHTX DSKBN RLCDS WNDQQ TJHRJ BURBT HTTPR YPRPK LLKPT EQKQC TIKPQ
BTJTN RHAKN IKAWN DQDJB WCDSC DJSHU ETPQC DJBPH DGTQC TJKJV TNORH DJPQN USQDK
JPKJY KUNDG TRAHR QLRSG P

3. Use the Vigenère Cipher, as described in Singh Chapter 2, to encipher the message "the man in the iron mask" using the keyword LOUIS.

4. The same plaintext message was enciphered using four different cipher techniques. A frequency analysis of each of the four resulting ciphertexts was conducted and the results graphed (see following pages). Match each frequency analysis with the cipher technique that produced it. *In a sentence or two, justify each of your answers.*

    a. Shift cipher +6 (the one that replaces "a" with "G")

    b. Shift cipher -10 (the one that replaces "a" with "Q")

    c. Transposition cipher
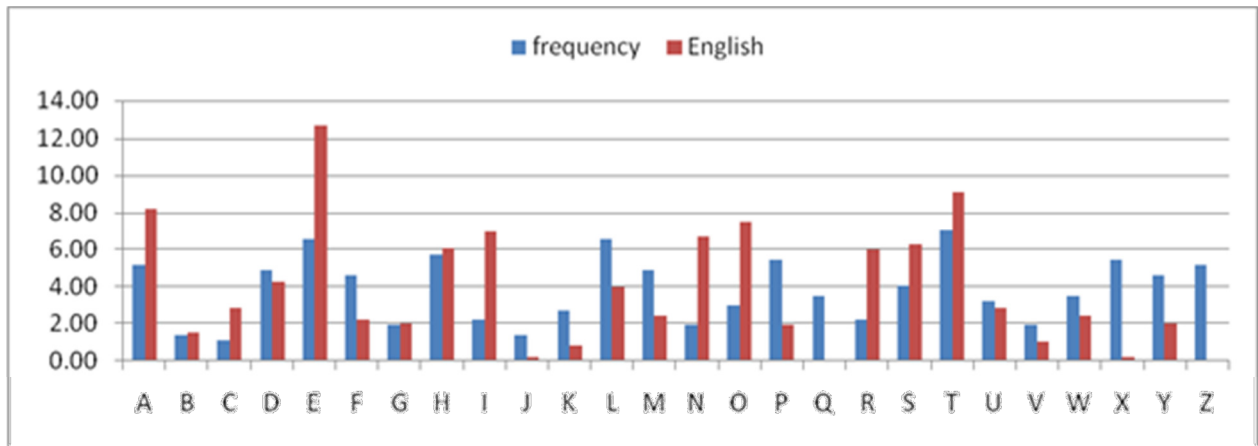
    d. Vigenère cipher

Frequency Analysis #1:

Frequency Analysis #2:

Frequency Analysis #3:

Frequency Analysis #4: